



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/473,522	12/28/1999	KENNETH A. PARULSKI	78744PRC	1080
1333	7590	02/09/2005	EXAMINER	
PATENT LEGAL STAFF EASTMAN KODAK COMPANY 343 STATE STREET ROCHESTER, NY 14650-2201			GYORFI, THOMAS A	
			ART UNIT	PAPER NUMBER
			2135	

DATE MAILED: 02/09/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/473,522	PARULSKI ET AL.	
	Examiner	Art Unit	
	Tom Gyorfi	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 19 October 2004.

2a) This action is FINAL. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-21 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 1-21 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) All b) Some * c) None of:

1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413)
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date. _____.
3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.	5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)
	6) <input type="checkbox"/> Other: _____.

DETAILED ACTION

1. Claims 1-15 were pending. The communication filed 10/19/04 amended claims 1-4 and 6-10, and added claims 16-21. Claims 1-21 remain for examination.

Response to Arguments

2. Applicant's arguments with respect to claims 1-21 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1 and 6-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Safai et al. (U.S. Patent 6,167,469), and further in view of Silverbrook (U.S. Patent 6,788,336).

Referring to Claim 1:

Safai discloses a digital camera of the type employing a private key to encrypt a hash of a digital image captured by the digital camera to produce an image authentication signature, the improvement comprising: (a) a processor

located within the digital camera for generating private key and a public key (col. 4, lines 1-15; col. 7, lines 30-40; Claim 29); and (b) means for storing the private key in a memory in the digital camera for subsequent use in encryption of the hash of the digital image to produce the image authentication signature (col. 16, lines 1-10, 20-35).

Safai does not explicitly teach "generating a random seed and for using the random seed to generate a private key and a public key."

Silverbrook discloses a processor located within a digital camera that generates a random seed (col. 189, lines 45-55) and teaches using a random seed to generate keys (col. 151, lines 12-13).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Silverbrook regarding a digital camera generating a random seed and using the random seed to generate keys into the digital camera disclosed by Safai in order to allow it to create the required public and private keys. The motivation for doing so would be to potentially increase the security of the camera by generating keys that cannot be easily compromised by guessing (col. 153, 15-20).

Referring to Claim 6:

Safai discloses a method of producing an image authentication signature in a digital camera employing a private key to encrypt a hash of an image captured by the digital camera, the improvement comprising the steps of:

(a) generating a private key in the digital camera (col. 4, lines 1-15; col. 7, lines 30-40; Claim 29); and

(b) storing the private key in a memory in the digital camera for subsequent encryption of the hash of the digital image (col. 16, lines 1-10, 20-35).

Safai does not explicitly teach "generating a random seed in the digital camera and using the random seed to generate a private key and a public key."

Silverbrook discloses generating a random seed (col. 189, lines 45-55) and using a random seed to generate keys (col. 151, lines 12-13).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Silverbrook regarding a digital camera generating a random seed and using the random seed to generate keys into the digital camera disclosed by Safai in order to allow it to create the required private key. The motivation for doing so would be to potentially increase the security of the camera by generating keys that cannot be easily compromised by guessing (col. 153, 15-20).

Referring to Claim 7:

Safai discloses a method of authenticating an image captured by a digital camera, comprising the steps of:

(a) generating a private key and a public key in the digital camera (col. 4, lines 1-15; col. 7, lines 30-40; Claim 29);

- (b) storing the private key in a memory in the digital camera (col. 16, lines 1-10, 20-35);
- (c) communicating the public key to a user (col. 4, lines 5-15);
- (d) capturing a digital image (col. 5, lines 35-45; col. 15, lines 60-65);
- (e) hashing the captured digital image in the digital camera to produce an image hash (col. 16, lines 1-10);
- (f) encrypting the image hash in the digital camera with the private key to produce a digital signature (col. 16, lines 20-35); and
- (g) authenticating the digital image by hashing the image outside of the digital camera, decrypting the digital signature using the public key to produce a decrypted signature, and comparing the decrypted signature with the image hash produced outside of the digital camera (col. 16, lines 10-20);

Safai does not explicitly teach “generating a random seed in the digital camera and using the random seed to generate a private key and a public key.”

Silverbrook discloses generating a random seed (col. 189, lines 45-55) and using a random seed to generate keys (col. 151, lines 12-13).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Silverbrook regarding a digital camera generating a random seed and using the random seed to generate keys into the digital camera disclosed by Safai in order to allow it to create the required public key and private key. The motivation for doing so would be to potentially increase the security of the camera by generating keys that cannot be easily compromised by guessing (col. 153, 15-20).

Referring to Claim 8:

Safai discloses a method of manufacturing a digital camera capable of producing a digital signature useful for image authentication, comprising the steps of:

- (a) manufacturing a digital camera with an internal processor for generating a public key and private key, storing the private key in a memory in the digital camera and communicating the public key to a camera operator;
- (b) sending the digital camera to an authentication service;
- (c) activating the digital camera at the authentication service to produce the public key and private key, and registering the public key at the authentication service; and
- (d) sending the digital camera to a user.

Safai does not explicitly teach “generating a random seed in the digital camera and using the random seed to generate a private key and a public key.”

Silverbrook discloses generating a random seed (col. 189, lines 45-55) and using a random seed to generate keys (col. 151, lines 12-13).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Silverbrook regarding a digital camera generating a random seed and using the random seed to generate keys into the digital camera disclosed by Safai in order to allow it to create the required private key. The motivation for doing so would be to potentially increase the security of the camera by generating keys that cannot be easily compromised by guessing (col. 153, 15-20).

Referring to Claim 9:

Safai discloses a digital camera of the type employing a private key to encrypt a hash of a digital image captured by the digital camera to produce an image authentication signature and a metadata signature corresponding to one or more metadata values, the improvement comprising:

(a) a processor located within the digital camera for generating a public key and a private key (col. 4, lines 1-15; col. 7, lines 30-40; Claim 29);

and

(b) means for storing the private key in a memory in the digital camera for subsequent use in encryption of the hash of the digital image to produce the image authentication signature and the metadata signature (col. 16, lines 1-10, 20-35).

Safai does not explicitly teach "generating a random seed in the digital camera and using the random seed to generate a private key and a public key."

Silverbrook discloses generating a random seed (col. 189, lines 45-55) and using a random seed to generate keys (col. 151, lines 12-13).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Silverbrook regarding a digital camera generating a random seed and using the random seed to generate keys into the digital camera disclosed by Safai in order to allow it to create the required private key. The motivation for doing so would be to potentially increase the security of the camera by generating keys that cannot be easily compromised by guessing (col. 153, 15-20).

Referring to Claim 10:

Safai discloses a method of producing an image authentication signature in a digital camera, comprising the steps of:

- (a) capturing a digital image (col. 15, lines 60-65);
- (b) compressing the captured digital image (col. 14, lines 15-25);
- (c) generating, a public key and private key in the digital camera (col. 4, lines 1-15; col. 7, lines 30-40; Claim 29);
- (d) storing the private key in a memory in the digital camera (col. 16, lines 1-10, 20-35);
- (e) providing one or more metadata values (col. 16, lines 1-15);
- (f) hashing the compressed captured digital image and at least one of the metadata values to produce an image hash (col. 16, lines 1-10); and
- (g) encrypting the image hash to produce the image authentication signature (col. 16, lines 20-30).

Safai does not explicitly teach “generating a random seed in the digital camera and using the random seed to generate a private key and a public key.”

Silverbrook discloses generating a random seed (col. 189, lines 45-55) and using a random seed to generate keys (col. 151, lines 12-13).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teachings of Silverbrook regarding a digital camera generating a random seed and using the random seed to generate keys into the digital camera disclosed by Safai in order to allow it to create the required private key. The motivation for doing so would be to potentially increase

the security of the camera by generating keys that cannot be easily compromised by guessing (col. 153, lines 15-20).

Referring to Claim 11:

Safai in view of Silverbrook discloses the limitations of Claim 10 above. Safai further discloses storing in an image file in the digital camera, the image authentication signature, the compressed digital image data, and the one or more metadata values (col. 12, lines 1-15; col. 14, lines 10-25; col. 16, lines 1-10).

Referring to Claim 12:

Safai in view of Silverbrook discloses the limitations of Claim 10 above. Safai further discloses the encrypting step includes encrypting the image hash with a private key produced in the digital camera to produce the image authentication signature (col. 16, lines 1-40).

Referring to Claim 13:

Safai in view of Silverbrook discloses the limitations of Claim 10 above. Safai further discloses wherein the encrypting step includes encrypting the image hash with the private key to produce the image authentication signature (col. 16, lines 25-40); and further including the step of:

authenticating the captured digital image by hashing the compressed digital image outside of the digital camera, decrypting the image authentication signature using the public key to produce a decrypted signature, and comparing

the decrypted signature with the image hash produced outside of the digital camera (col. 16, lines 10-25).

Referring to Claim 14:

Safai in view of Silverbrook discloses the limitations of Claim 1 above. Safai further hashing the uncompressed captured digital image to produce a random number k (col. 16, lines 1-10); and wherein the encrypting step includes using the random number k to produce the image authentication signature (col. 16, lines 20-35).

Referring to Claim 15:

Safai in view of Silverbrook discloses the limitations of Claim 1 above. Safai further discloses the encrypting step further produces a metadata signature corresponding to the one or more metadata values (col. 16, lines 1-10; col. 12, lines 50-60).

Regarding claims 16-21:

Safai in view of Silverbrook discloses the limitations of Claims 1 and 6-10 above. Safai also discloses firmware memory, wherein the private key is produced using an algorithm stored in the firmware memory (col. 7, lines 50-55).

Neither Safai nor Silverbrook explicitly disclose “wherein the algorithm is deleted from the firmware memory after the private key is generated.” However, Silverbrook teaches that an attacker could gain control of the program [algorithm]

used to generate a random seed and use it to reverse engineer a private key, while not being authorized to do so (col. 155, line 55-60). This suggests that it would be desirable to delete the algorithm used to generate a private key after the unique private key for a digital camera has been generated. Thus, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination of Safai and Silverbrook to delete the algorithm from the firmware memory after the private key is generated, in order to prevent it from falling into the wrong hands.

5. Claims 2-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Safai and Silverbrook as applied to claim 1 above, and further in view of Glass et al. (U.S. Patent 6,332,193).

Referring to Claim 2:

Safai in view of Silverbrook discloses the limitations of Claim 1 above. Safai further discloses an image sensor for capturing images (col. 5, lines 30-40).

Neither Safai nor Silverbrook explicitly disclose "the processor includes means for producing a random seed for the private key by processing an image captured from the image sensor so that the random noise level in the captured image is used in producing the random seed".

Glass discloses the processor includes means for producing a random seed for the private key processing an image captured from the image sensor so that the random noise level in the captured image is used in producing [the

random seed, by hashing an initial test image captured by the digital camera] (col. 4, lines 1-10).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify the teachings of Safai and Silverbrook such that the random seed used to generate the private key is generated based on sensor information, as suggested by Glass. One of ordinary skill in the art would have been motivated to do this because it would provide a private key that is easily changed and random.

Referring to Claim 3:

The combination of Safai, Silverbrook, and Glass discloses the limitations of Claim 2 above. Safai further discloses

- (i) a variable gain amplifier coupled to the image sensor (col. 5, lines 45-60);
- (ii) an analog-to-digital converter coupled to the variable gain amplifier and the processor for producing digital signals corresponding to the captured images (col. 5, lines 50-60); and
- (iii) the processor causing the variable gain amplifier to be in a high gain condition when the initial test image is captured (col. 5, lines 55-60).

Referring to Claim 4:

Safai in view of Silverbrook discloses the limitations of Claim 1 above.

Neither Safai nor Silverbrook explicitly discloses "the processor includes one or more algorithms for producing a random seed, wherein the random seed is used to produce a random number k, and for using the random number k to create the image authentication signature by hashing the raw image data prior to image processing."

Glass discloses the processor includes one or more algorithms for producing the random seed, wherein the random seed is used to produce a random number k, and for using the random number k to create the image authentication signature by hashing the raw image data prior to image processing (col. 3, line 60-col. 4, line 15).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to modify Safai in view of Silverbrook such that authentication is applied to an image using a random number. One of ordinary skill in the art would have been motivated to do this because it would allow the user to authenticate the image (col. 3, lines 60-65).

Referring to Claim 5:

The combination of Safai, Silverbrook, and Glass discloses the limitations of Claim 4 above. Safai further discloses the processor includes an image processing algorithm which uses JPEG compression (col. 14, lines 15-25).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tom Gyorfi whose telephone number is (571) 272-3849. The examiner can normally be reached on 8:00am - 4:30pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

TAG
1/28/05



KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2